UNIVERSIDAD
COMPLUTENSE
MADRID

Proyecto de Innovación

Convocatoria 2020/2021

Nº del proyecto: 41

Infraestructura para la expansión de escenarios de guerra digital como apoyo a la docencia en ciberseguridad

Responsable del proyecto:
José Luis Vázquez Poletti

Facultad de Informática

Departamento Arquitectura de Computadores y Automática

1 Objetivos propuestos en la presentación del proyecto

El objetivo de este proyecto ha sido dotar al alumnado de un entorno persistente donde realizar ejercicios de ciberseguridad, extendiendo la infraestructura ya disponible en los laboratorios de la Facultad de Informática, pero limitada en el tiempo de acceso a los mismos.

Para ello, el proyecto se centra en los siguientes aspectos:

- Despliegue del entorno de entrenamiento en un equipo centralizado mediante la aplicación de mecanismos de virtualización.
- Crear un repositorio de escenarios de entrenamiento (mediante máquinas virtuales) que se puedan desplegar de manera individual.
- Elaboración de un protocolo o mecánica de conexión para el estudiante.

2 Objetivos alcanzados

A continuación se indica el nivel de completitud de cada objetivo,

2.1 Despliegue de una solución de virtualización en la máquina que se hubiera adquirido a través del proyecto de innovación docente

Completada, salvo por el hecho de que la máquina no fue adquirida a mediante los fondos asignados para el proyecto de innovación (0 euros), sino por el reciclaje de una perteneciente a otro proyecto.

2.2 Creación de un repositorio de máquinas virtuales vulnerables para un despliegue selectivo

Completada. Se han suministrado dos máquinas virtuales vulnerables con diferentes ambientaciones, activando una para cada cuatrimestre.

2.3 Elaboración de un protocolo o mecánica de conexión para el estudiante

Completada. Se ha utilizado el mismo protocolo que en las actividades de *pentesting* del Grupo de Hacking Ético de la Facultad de Informática[1].

3 Metodología empleada en el proyecto

El proyecto se dividió en las siguientes tareas:

- T1. Preparación del sistema base.
- T2. Preparación de máquinas virtuales idóneas.
- T3. Implementación del sistema de acceso.
- T4. Despliegue en pruebas.
- T5. Despliegue en producción.

Si bien estas tareas se concibieron como secuenciales, se admite un cierto nivel de solapamiento entre T1, T2 y T3.

[1] https://fdist.ucm.es/

4 Recursos humanos

El equipo de trabajo que forma este proyecto es el siguiente:

- José Luis Vázquez (JLV, jlvazquez@fdi.ucm.es): doctor en informática, director de la Oficina de Software Libre y Tecnologías Abiertas de la UCM[2] y coordinador del grupo de hacking ético de la Facultad de Informática.
- Juan Carlos Fabero (JCF, jcfabero@ucm.es): doctor en física, subdirector del Departamento de Arquitectura de Computadores y Automática, y coordinador del grupo de hacking ético de la Facultad de Informática.
- Iván Martínez (IM, imartinez@fdi.ucm.es): doctor en informática y ex-asesor del vicerrector de nuevas tecnologías.
- David Pacios (DP, dpacios@ucm.es): estudiante de la Facultad de Informática, colaborador de la Oficina de Software Libre y Tecnologías Abiertas de la UCM, presidente (saliente) de la asociación ASCII.
- Fernando Méndez (FM, fernmend@ucm.es): estudiante de la Facultad de Informática, colaborador de la Oficina de Software Libre y Tecnologías Abiertas de la UCM, presidente (saliente) de la asociación Diskóbolo.

Todos los miembros del proyecto han sido indispensables en prácticamente todas las tareas del mismo. Concretamente, JLV, JCF e IM aportaron su experiencia en estas tecnologías en las tareas T1, T2, T3 y T5. Por otro lado, DP y FM, desde su punto de vista de usuarios finales, aportaron muchísimo a las tareas T2 y T4, aunque por supuesto demostraron estar ampliamente capacitados para participar en el resto de las tareas, y así lo hicieron.

5 Desarrollo de las actividades

5.1 Despliegue de la infraestructura

La máquina física empleada dispone de 8 procesadores Intel Xeon E31240, 8GB de memoria RAM y 200GB de disco duro. Se encuentra alojada en la Facultad de Informática.

El sistema operativo es Ubuntu Linux 20.04.01 LTS[3]. El hipervisor elegido es VirtualBox[4], gratuito y de código abierto.

La gestión de la máquina física se realiza a través de SSH en un puerto diferente al estándar y VNC, activado bajo demanda. Las imágenes de las máquinas virtuales son subidas a la máquina física a través de SFTP. La gestión de las máquinas virtuales se realiza mediante los comandos *vbox**.

Las máquinas virtuales se van desplegando, una cada vez, con redirección completa de puertos, salvo para los de gestión (SSH y VNC).

Esta infraestructura se ha puesto en marcha durante el mes de septiembre de 2020.

5.2 Conexión a la infraestructura

Al encontrarse en la red de la UCM y realizarse actividades de *pentesting*, se vio necesario racionalizar el acceso.

Por ello, la máquina sólo es accesible para los ataques a través de la VPN suministrado por Servicios Informáticos de la UCM al Grupo de Hacking Ético de la Facultad de Informática. Para hacer uso de la misma, es necesario registrarse en el grupo previamente.

[2] https://www.ucm.es/oficina-de-software-libre/

[3] https://releases.ubuntu.com/20.04/

[4] https://www.virtualbox.org/

Figure 1: Carta usada durante la promoción de la máquina "Cubo Borg".

Figure 2: Carta usada durante la promoción de la máquina "Ministerio del Tiempo".

5.3 Máquinas virtuales desplegadas

Durante el curso 2020/2021 se han ofrecido dos máquinas virtuales, una en cada cuatrimestre. La mecánica siempre es la misma: tanto en el directorio *$HOME* del usuario principal como en el del *root* (administrador) existe un fichero con una clave que debe ser enviado a una dirección de correo.

Estas máquinas son:

- **Cubo Borg.** Una máquina cuyo acceso con un usuario regular requiere de ciertas dotes de *footprinting* del atacante. La escalada de privilegios posterior va cronometrada, puesto que el sistema expulsa al usuario pasado un tiempo.
- **Ministerio del Tiempo.** Basada en una máquina existente con múltiples vulnerabilidades, su principal dificultad es que su cortafuegos impide el acceso a los puertos abiertos de forma aleatoria cada cierto tiempo.

Durante el curso 2020/2021, el Cubo Borg fue vulnerado completamente por 3 estudiantes[5] y el Ministerio del Tiempo por 4 estudiantes[6].

A lo largo del periodo de prueba, los estudiantes han mostrado interés por la actividad y han podido afianzar los conocimientos adquiridos en clase.

[5] https://twitter.com/FDI_st/status/1325771758952189954
[6] https://twitter.com/FDI_st/status/1385166710534283265